Pacific Northwest
NATIONAL LABORATORY
*Proudly Operated by Battelle Since 1965*

# HONE: Correlating Host activities to Network communications to produce insight

**What if you could collect and analyze only the most important cyber security data?**


GLENN A. FINK, PH.D.
Senior Scientist, Secure Cyber Systems

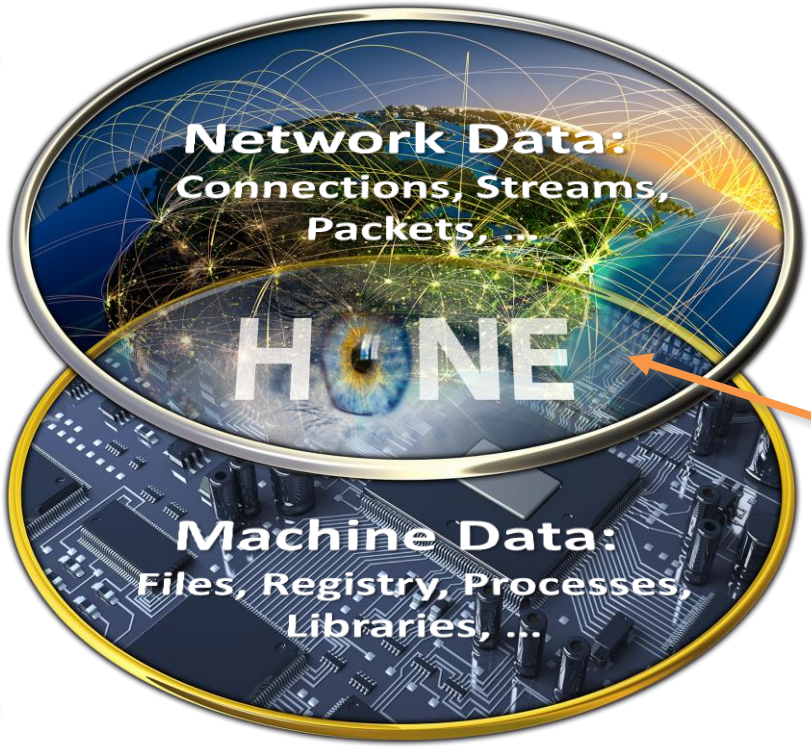
SEAN STORY, PMP
Project Manager, Software Engineering & Architectures

# What is the problem?



- We collect too much extraneous cyber data and then put in too much work to process it all

We collect both network and machine data



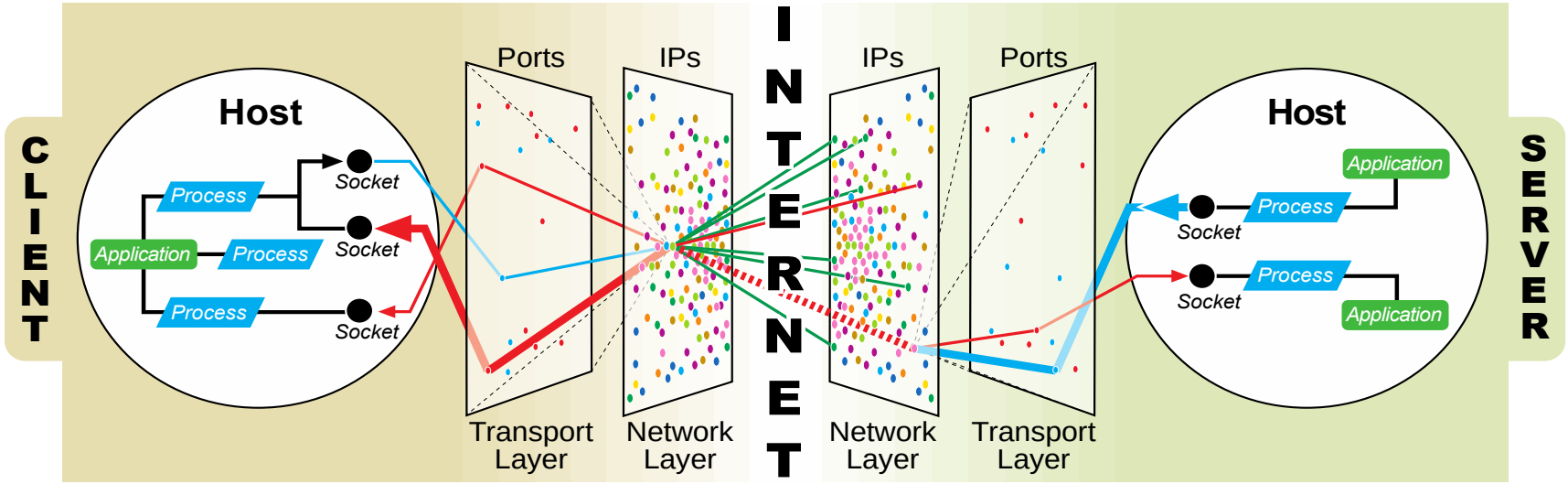

But we only need the correlated intersection

- Why? The design of Internet protocols makes correlation and isolating root causes of break-ins difficult

# How will we fix the problem?



- We *correlate* communications and processing activities in the kernel of the operating system
- This lets us find out what programs are responsible for malicious network activity




- Requires a kernel module on each monitored machine

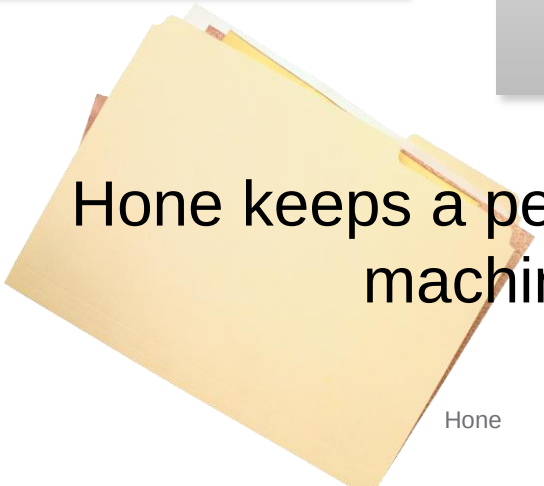
# What are the benefits?



Fewer analyst hours are needed to correlate cyber data → savings

Analysts can characterize communications with 100% accuracy

Hone provides a key to understand the computer from the network



Hone keeps a persistent file of correlated machine and network activities

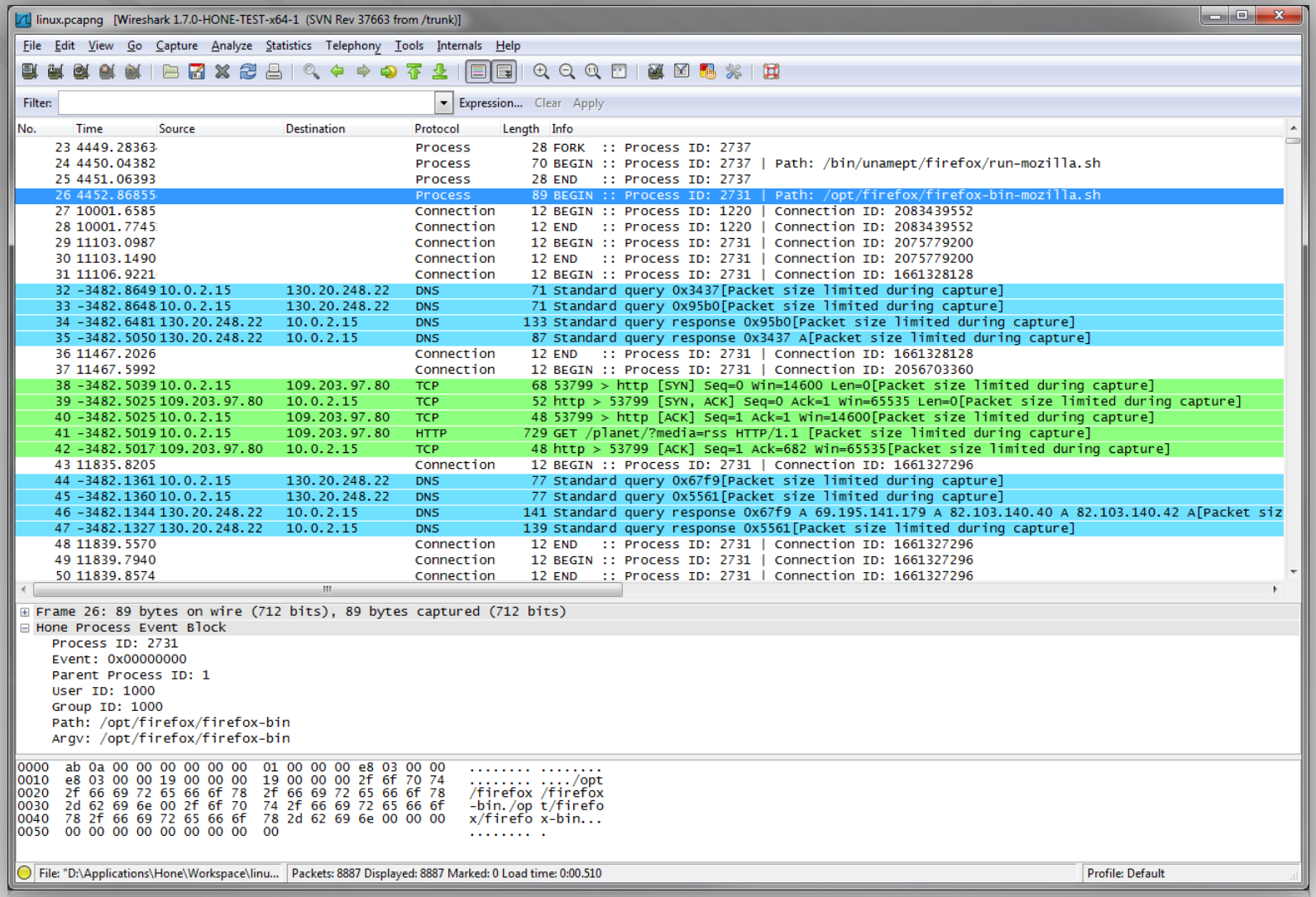
# What alternatives are there?



- TCPView, NetStat, and other host-based tools:
  - Can see the connections but not the actual activity
  - Use a polling approach that misses short events
- Deep-packet inspection or Dynamic Analysis
  - Expensive and potentially inaccurate
- Connection-filtering host-based firewalls
  - Only operate on the connection level, not per packet
  - Once you grant blanket permission to an application, you have no further control
- Multi-host-based security and analysis
  - Requires elaborate infrastructure

# Hone Demonstration

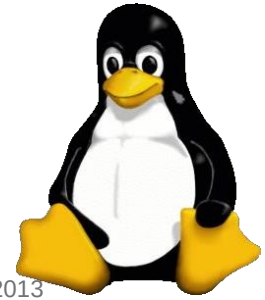
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965



# Conclusion



- All Internet devices use common protocols, so Hone's simple correlation will enable a revolution in defense
- Hone provides the precision to control communications at the packet level
- Hone gives trustworthy process attribution
- We are seeking partners to:
  - Sponsor follow-on work
  - Test deploy operational prototypes
  - License for use in new and existing products



# Correlating machine and network activities to produce insight

Pacific Northwest NATIONAL LABORATORY
*Proudly Operated by Battelle Since 1965*






**Glenn Fink, PhD**
Cyber Security Scientist
Glenn.Fink@pnnl.gov
(509) 375-3994




**Sean Story, PMP**
Project Manager
story@pnnl.gov
(509) 375-3612

Pacific Northwest National Laboratory
Richland, Washington